Washington Law Review

Volume 74 | Number 2

4-1-1999

Washington's "Spam-Killing" Statute: Does It Slaughter Privacy in the Process?

Steven Miller

WASHINGTON'S "SPAM-KILLING" STATUTE: DOES IT SLAUGHTER PRIVACY IN THE PROCESS?

Steven Miller

Abstract: In 1998, the Washington Legislature passed an historic law prohibiting the sending of commercial e-mail messages containing false or misleading information in the subject line or header. The law also permits companies that provide Internet services, known as Internet Service Providers (ISPs), to block the transmission or receipt of messages reasonably believed to violate the statute. However, the law fails to specify the permissible activities that an ISP may pursue to form such a reasonable belief. It thereby encourages a variety of intrusive ISP activities, such as message screening. Existing statutory and constitutional privacy law provides the only shield for an e-mail subscriber against invasive ISP activities. This Comment argues that these existing privacy laws fail to provide meaningful protection to e-mail subscribers from the potential abuses of their ISPs. The Comment recommends legislative action to amend the anti-spam law by explicitly limiting the ways in which an ISP may develop its "reasonable belief" that a particular e-mail message violates the anti-spam statute.

Samantha begins typing an electronic mail, or e-mail, to her business partner, Roger, outlining her latest ideas about their plan to found an Internet start up company that would offer innovative new services over the World Wide Web. She titles the message "A few more thoughts about our new company." At the end of the message, Samantha quickly reminds Roger that she is in the market for a new computer and that she would gladly sell her old computer to him for a decent price. Samantha clicks the "send" button on her e-mail browser and assumes that Roger will receive the message without delay or inspection.

The message travels across the Internet to Roger's Internet Service Provider (ISP),[1] but unknown to Samantha or Roger, the ISP saves a copy of the message for delivery. The ISP then examines the contents of the saved message, including Samantha's private statements about their new Internet company. Based on Samantha's comment about selling her computer, the ISP determines that the message constitutes commercial e-mail containing a false or misleading subject line. The ISP then directs the message into cyberspace limbo.

---

1. An ISP is a company or organization that provides its subscribers with access to the Internet. Typically, the ISP also furnishes each subscriber with a private e-mail account, although this is not always the case. *See* Learn the Net, *LEARN THE NET: How E-mail Works* (last modified Mar. 22, 1999) <http://www.learnthenet.com/english/html/20how.htm>. This Comment treats ISPs and e-mail service providers identically.

Samantha reasonably assumes that Roger received the message. Roger, on the other hand, wonders why Samantha has taken so long to respond to his last e-mail. Meanwhile, Roger's ISP is apprised of Samantha and Roger's innovative ideas for an Internet startup company. Nevertheless, Samantha and Roger may be statutorily precluded from seeking legal relief against the ISP for injuries stemming from the ISP's monitoring and blocking activities.

In 1998, the Washington Legislature enacted a statute that purports to increase the privacy of the e-mail inbox by protecting it from false or misleading commercial e-mail messages, but actually diminished users' privacy in the messages they send and receive. The statute,[2] commonly known as the Washington "anti-spam" law,[3] attempts to curb unwanted e-mail by prohibiting the initiation of commercial e-mail that either misrepresents the origin of the message or contains misleading information in the subject line. The statute also permits those injured by such e-mail to initiate civil suits against the sender. These provisions provide privacy protection for e-mail consumers against unwanted fraudulent e-mail.

The statute also permits ISPs to block the transmission or receipt of messages they reasonably believe violate the statute. Because the statute requires that an ISP must reasonably believe that an e-mail message violates the statute before blocking the e-mail, the statute implicitly encourages ISPs to examine the contents of messages to form that reasonable belief. The statute also relieves ISPs from liability for blocking the transmission or receipt of such messages when ISPs do so in good faith.

Part I of this Comment provides an overview of the existing anti-spam law. Part II summarizes statutory and constitutional privacy rights that are relevant to e-mail subscriber privacy. Part III describes three possible courses of action that an ISP might take to enforce its statutory right to block violative messages. Part IV argues that the existing statutory and constitutional privacy rights provide e-mail subscribers with inadequate protection from highly intrusive ISP courses of action. Part V

2. 1998 Wash. Laws 149 (codified as amended at Wash. Rev. Code § 19.190.005 (1998)).

3. The word "spam" is a derisive label for unwanted commercial e-mail messages. Indeed, the word has such negative connotations that the Hormel Foods Company, manufacturer of a processed meat product with the same name, sued to enjoin the use of the word on a commercial web site. Hormel's efforts in court were unsuccessful. Laurie J. Flynn, *Gracious Concession on Internet 'Spam,'* N.Y. Times, Aug. 17, 1998, at D3.

recommends amendment of the Washington anti-spam law to prohibit ISPs from actively monitoring the content of messages. It further recommends permitting ISPs to block messages only in response to past subscriber complaints. This approach will improve the protection of subscribers from the intrusive actions of ISPs without substantially diluting the protection that the legislature intended to provide ISPs.

I. WASHINGTON'S ANTI-SPAM STATUTE

A. The Impetus for a Statutory Solution

E-mail is quickly becoming a profoundly important tool of communication. One analyst estimates that there are nearly 200 million active e-mail accounts worldwide.[4] Two factors contributing to the astonishing growth of e-mail communication are its blindingly fast speed and extremely low cost.[5] However, not unlike the traditional mailbox, advertisements have increasingly saturated the e-mail inbox.[6] Technologically savvy entrepreneurs, alert to the potential for profit from the technology and the captive audience of e-mail subscribers, have responded by sending large quantities of commercial electronic messages to those subscribers.[7]

Commercial bulk e-mailing has frustrated e-mail subscribers. The practice has also substantially burdened the companies that provide Internet access, ISPs. The Internet depends on the cooperative efforts of computer network operators who "independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers)."[8] Once a user sends an e-mail

4. Deborah Branscum, *King of 'Spam' and Proud of It*, Newsweek, May 12, 1997, at 90, 90.

5. Most e-mail subscribers pay either a flat fee for unlimited access or a per-hour rate for Internet access. Subscribers typically do not pay any per-message costs, and therefore, the marginal cost of sending e-mail messages is low. CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1018 (S.D. Ohio 1997). Many users also have access to e-mail through their employment or school and do not personally pay for those e-mail services.

6. One entrepreneur allegedly sent between 100,000 and 1,000,000 unsolicited e-mail messages per week advertising a book about making money on the Internet. Peter Lewis, *State Targets Oregon Man in First Anti-Spam Lawsuit*, Seattle Times, Oct. 22, 1998, at A1.

7. The only major cost that senders of bulk e-mail incur is the cost of obtaining lists of e-mail addresses to which they can send their messages. For a one-time start-up cost of about $1000, senders can purchase software that will harvest those e-mail addresses. Branscum, *supra* note 4, at 90.

8. ACLU v. Reno, 929 F. Supp. 824, 832 (E.D. Pa. 1996).

message over the Internet, computers relay the message from one Internet server to another until the message arrives at its intended destination. Thus, ISPs with no relationship to the sending or receiving parties act as postal carriers for these messages, and the computers of those ISPs shoulder the burden of forwarding the messages to their intended recipients.[9] Although foreign ISPs receive no reimbursement from the senders of bulk e-mail messages, they are nevertheless co-opted into service and exposed to potential computer overload from the highly concentrated volume of e-mail communication. Bulk e-mailers may also deliberately impose costs on foreign ISPs by falsifying the point of origin of their bulk e-mail messages.[10] Likewise, receiving ISPs incur substantial costs when the unwanted bulk e-mail messages arrive at their intended destinations, because the receiving ISPs must process and store the messages for delivery to the intended recipients.[11]

B. The Provisions of Washington's "Anti-Spam" Law

In March 1998, lawmakers in Washington unanimously voted to take action against abusive commercial e-mail practices when they enacted Washington's "anti-spam" law.[12] The law prohibits the initiation of commercial e-mail messages that misrepresent the source of the message[13] or contain false or misleading information in the subject line.[14]

---

9. This Comment uses the term "foreign ISP" to describe ISPs having no contractual relationship with either the sender or the recipient of an e-mail message.

10. For instance, a bulk e-mail sender may send a message that falsely purports to originate from an account with America Online, a national ISP. Because recipients of the message reasonably assume that the message originated with America Online, those recipients may send responses or complaints to America Online, which involuntarily assumes the cost of processing, storing, and responding to the complaints. America Online also receives any messages that are returned as undeliverable and bears the costs of processing those messages as well. America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998).

11. See, for example, *Cyber Promotions, Inc. v. American Online, Inc.*, 948 F. Supp. 436, 438 (E.D. Pa. 1996), in which America Online, a major ISP, complained that its e-mail servers were being overloaded by millions of e-mail messages that Cyber Promotions, a sender of unsolicited spam e-mail, was sending to America Online subscribers each day. America Online has estimated that it receives at least one million spam e-mail messages per day from various senders. William Baldwin, *Spam Killers*, Forbes, Sept. 21, 1998, at 254, 254.

12. The Act passed the Washington Senate with 42 yeas, zero nays and then passed the State House of Representatives with 96 yeas, zero nays. Certification of Enrollment, E.S.H.B. 2752, 55th Leg., Reg. Sess. (Wash. 1998). The Act is codified at Wash. Rev. Code § 19.190.005–.050 (1998).

13. The statute prohibits parties from sending commercial e-mails purporting to originate from "nobody@nowhere.com" when the e-mail actually originates from another e-mail account. *See infra* note 22 and accompanying text.

The legislature found that the growing volume of commercial e-mail and the accompanying burden on ISPs warranted immediate relief.[15]

The law originally proposed to combat spam would have directly prohibited unsolicited commercial e-mail messages,[16] but the version the legislature ultimately adopted indirectly regulates unsolicited e-mail by prohibiting commercial messages with false or misleading information.[17] The initial proposal faced a vigorous challenge from the American Civil Liberties Union (ACLU) because the proposal contained an "exceedingly broad definition of unsolicited commercial speech."[18] These protests from free speech supporters convinced the Washington Legislature to indirectly regulate unsolicited commercial e-mail by prohibiting false or misleading commercial e-mail.[19] The legislature apparently believed that regulating false or misleading commercial e-mail was more consistent with the First Amendment of the U.S. Constitution than completely prohibiting unsolicited commercial e-mail.[20]

The statute sets forth two distinct ways in which an e-mail message can violate the law.[21] First, the statute prohibits messages containing misleading point of origin information.[22] Thus, a message indicating that "nobody@nowhere.com" is the originating party of the e-mail violates the statute if the message originated from a different sender. Second, a

---

14. If the subject line claims "You've just won $1000!" but the content of the message instead promotes a "get rich quick" scheme, that message would violate the statute. *See infra* notes 23–24 and accompanying text.

15. Wash. Rev. Code § 19.190.005.

16. S.H.B. 2752, 55th Leg., Reg. Sess. (Wash. 1998). This was also the approach originally endorsed by the Attorney General. Attorney Gen. of Wash., *1998 Legislative Agenda* (visited Mar. 12, 1999) <http://www.wa.gov/ago/test/docket/story_vault/ 98_leg_agenda.html>.

17. *See* Wash. Rev. Code § 19.190.005–.050. A commercial e-mail message is one that is "sent for the purpose of promoting real property, goods, or services for sale or lease." Wash. Rev. Code § 19.190.010(1).

18. Peter Lewis, *Spam on Trial*, Seattle Times, June 7, 1998, at C1 (quoting ACLU's Jerry Sheehan).

19. *Id.*

20. *See, e.g.*, Florida Bar v. Went For It, Inc., 515 U.S. 618, 623–24 (1995) ("[T]he government may freely regulate commercial speech that concerns unlawful activity or is misleading.").

21. Wash. Rev. Code § 19.190.020(1).

22. The precise language of the statute prohibits the sending of any e-mail that "[u]ses a third party's internet domain name without permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path of a commercial electronic mail message." Wash. Rev. Code § 19.190.020(1)(a). Because using a third party's Internet domain name without permission is likely to misrepresent the point of origin, this Comment uses the phrase "misleading point of origin" to refer to both practices.

message also violates the statute if it contains false or misleading information in the subject line.[23] For example, if the subject line reads "You've just won $1000!" but the content of the message instead promotes a "get rich quick" scheme, the e-mail violates the statute.[24] Contrary to the original proposal, a message does not violate the statute merely because it is unsolicited commercial e-mail, nor is "solicited" e-mail necessarily immune from attack under the statute.[25]

Because the statute is state legislation, its scope is geographically limited.[26] Thus, messages with false or misleading information violate the statute only if they are sent from a computer located in Washington or to an e-mail account that the sender knows is held by a Washington resident.[27] For purposes of the statute, the sender of an e-mail message knows that the receiving party is a Washington resident if "that information is available, upon request, from the registrant of the internet domain name contained in the recipient's electronic mail address."[28]

The intended recipient and the receiving ISP may bring a civil action against violators to recover their damages, although the measure of their

23. Wash. Rev. Code § 19.190.020(1)(b).

24. A subject line contains false or misleading information if the subject line misrepresents the text contained in the body of the e-mail message. *See* Attorney Gen. of Wash., *Unsolicited E-mail* (visited Mar. 12, 1999) <http://www.wa.gov/ago/junkemail/verify.html>.

25. The Code titles for the sections that set forth the prohibitions on commercial e-mail messages both begin with the phrase "Unsolicited or misleading electronic mail." Wash. Rev. Code §§ 19.190.020 & .030 (1998). The Attorney General's web site also indicates that an ISP may block e-mail only once the ISP has reason to believe that its network is being used "to send unlawful *unsolicited* commercial e-mail." Attorney Gen. of Wash., *Unsolicited E-mail* (visited Mar. 12, 1999) <http://www.wa.gov/ago/junkemail/protect.html> (emphasis added). Although the original legislative proposal did define unsolicited e-mail as a violation, the prohibitions enacted by the legislature contain no language regarding unsolicited mail in either the titles or the text. *See supra* note 16 and accompanying text. Because there is a discrepancy between the Code version and the enacted version, the actual language of the legislative enactment trumps the codified version. State v. City of Mercer Island, 58 Wash. 2d 141, 144, 361 P.2d 369, 371 (1961) (holding that text of legislative enactment prevails over restatement thereof in Code).

26. A question exists as to whether the present statute impermissibly interferes with interstate commerce, in violation of the commerce clause of the U.S. Constitution. Lewis, *supra* note 18, at C1. Careful consideration of this issue is beyond the scope of this Comment.

27. Wash. Rev. Code § 19.190.020(1) (1998).

28. Wash. Rev. Code § 19.190.020(2) (1998). The Attorney General and the Washington Association of Internet Service Providers (WAISP) co-sponsor a statewide registry of e-mail accounts held by Washington residents. Washington e-mail subscribers can register their accounts by accessing the WAISP Registry Page. Washington Ass'n of Internet Serv. Providers, *WAISP Registry Page* (last modified Sept. 21, 1998) <http://registry.waisp.org>.

damages may differ.[29] The statute also declares that violations of the anti-spam law qualify as violations of the Consumer Protection Act.[30] As a result, the Attorney General may sue violators of the anti-spam law.[31] In addition, because an anti-spam statute violation is also a Consumer Protection Act violation,[32] recipients and ISPs may seek to recover attorneys' fees in their own actions for damages.[33]

Perhaps the most controversial portion of the law is the provision allowing ISPs to block voluntarily the transmission or delivery of e-mail that the ISP reasonably believes violates the statute.[34] The anti-spam statute relieves ISPs from liability if they block e-mail in good faith reliance on the statute.[35] The statutory text does not, however, limit or define the ways in which an ISP may form the requisite reasonable belief. This gap in the statute exposes e-mail subscribers to numerous potential privacy invasions by their ISPs.

II. EXISTING PRIVACY PROTECTIONS RELEVANT TO E-MAIL MESSAGES

Federal and state laws presently provide some communications privacy protection. The Federal Electronic Communications Privacy Act protects electronic communications from unauthorized interception, access, and disclosure.[36] The Washington Constitution protects the privacy right in decisionmaking and in nondisclosure of personal

29. Damages for e-mail subscribers are presumptively set at $500 per e-mail, but subscribers may recover actual damages if they are greater than the presumed amount. ISPs are presumed to suffer $1000 per violative e-mail, but may recover actual damages if they exceed the presumed amount. Wash. Rev. Code § 19.190.040 (1998).

30. A violation of the anti-spam law is "an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86." Wash. Rev. Code § 19.190.030(2) (1998).

31. Wash. Rev. Code § 19.86.080 (1998). The Washington Attorney General first exercised this power in October 1998 by filing an action against an Oregon man who allegedly sent violative commercial e-mail messages. Lewis, *supra* note 6, at A1.

32. *See supra* note 30.

33. Parties injured by unfair methods of competition or by unfair or deceptive acts of trade may seek reasonable attorney's fees. Wash. Rev. Code § 19.86.090 (1998); *see also* Attorney Gen. of Wash., *Unsolicited E-mail* (visited Mar. 12, 1999) <http://www.wa.gov/ago/junkemail/action.html> (indicating that recipients of violative e-mail messages may be eligible to recover attorney's fees).

34. Wash. Rev. Code § 19.190.050(1) (1998).

35. Wash. Rev. Code § 19.190.050(2) (1998).

36. *See infra* Part II.A.

information.[37] The Washington Privacy Act, which predates the anti-spam law, prohibits unauthorized parties from opening or reading sealed messages and also forbids the use of a device to record or intercept point-to-point communications.[38]

A. The Federal Electronic Communications Privacy Act

In 1986, Congress amended the Federal Wiretap Act by passing the Electronic Communications Privacy Act (ECPA).[39] The ECPA prohibits unauthorized interception of electronic communications during their transmission,[40] disallows unauthorized access to or interference with electronic communications while they are in storage,[41] and forbids electronic communication service providers from divulging the contents of stored electronic communications.[42] Violators are subject to civil suit for damages,[43] and under certain circumstances may be subject to fines, imprisonment, or both.[44]

Although the ECPA does not expressly mention e-mail,[45] the statutory language does protect "electronic communication."[46] Several courts have concluded that the statutory protection encompasses e-mail messages.[47] The legislative history of the statute also strongly indicates that the legislature anticipated that the ECPA protections against interception,

---

37. *See infra* Part II.B.

38. *See infra* Part II.C.

39. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2510 (1994)).

40. 18 U.S.C. § 2511 (1994).

41. 18 U.S.C. § 2701 (1994).

42. 18 U.S.C. § 2702 (1994).

43. The statute authorizes actions for civil damages for interception of electronic messages pursuant to 18 U.S.C. § 2520 (1994), and for unauthorized access or distribution of such messages pursuant to 18 U.S.C. § 2707 (1994).

44. Fine and/or imprisonment may serve as the penalties for unauthorized interception or access. 18 U.S.C. §§ 2511(4), 2701(b) (1994).

45. Jennifer C. Dombrow, Note, *Electronic Communications and the Law: Help or Hindrance to Telecommuting?*, 50 Fed. Comm. L.J. 685, 696 (1998).

46. Electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (1994).

47. *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998); Wesley College v. Pitts, 974 F. Supp 375, 381 (D. Del. 1997); State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc., 909 F. Supp 137, 145 (S.D.N.Y. 1995).

access, and disclosure would protect e-mail messages.[48] Because the ECPA's provisions regarding interception, access, and disclosure are subject to varying rules and exceptions,[49] the following discussion treats each provision separately.

1. Interception of Electronic Communications During Transmission

The ECPA prohibits interception, which is defined as the "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device."[50] This prohibition on interception applies to electronic communication only at the time of transmission and does not apply once messages have been stored for later retrieval.[51] Furthermore, this provision only prevents acquisition of the contents of the messages.[52] The provision does not protect other information contained in an electronic communication, such as the identity of the sending party of an e-mail message.[53]

Acquisition of the contents of an electronic communication that would otherwise constitute an "interception" might nonetheless fall under one of the statutorily enumerated exceptions. The ECPA permits interception of an electronic communication when one of the parties to the communication has given prior consent to such interception.[54] In addition, electronic communication service providers are permitted to intercept or use electronic communications in a manner that is necessary to provide service or to protect the rights or property of the service provider.[55]

---

48. *See* S. Rep. No. 99-541, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568 (recognizing that ECPA does not explicitly address e-mail messages, but that scope of statute encompasses electronic mail, digitized transmissions, and video teleconferences).

49. *See, e.g.*, Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (distinguishing between protection from interception during transmission under 18 U.S.C. § 2511 and protection of stored communications under §§ 2701–11); *State Wide*, 909 F. Supp. at 145 (S.D.N.Y. 1995) (distinguishing between access to stored electronic communications and disclosure of stored communications).

50. 18 U.S.C. § 2510(4) (1994).

51. *Bohach*, 932 F. Supp. at 1235–36.

52. The ECPA defines "contents" with respect to electronic communication as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (1994).

53. Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (interpreting ECPA's definition of "contents" as not extending to identity of sending party of e-mail message).

54. 18 U.S.C. § 2511(2)(c)–(d) (1994).

55. 18 U.S.C. § 2511(2)(a)(i) (1994).

2. *Disclosure of Stored Electronic Communications*

A second provision of the ECPA specifically addresses electronic communications service providers and prohibits those providers from disclosing the contents of electronic communications in storage.[56] Under the statute, providers of electronic communications services may not knowingly divulge to any person or entity the contents of a stored communication.[57] While this provision prohibits disclosure of the contents of a message, it does not prohibit disclosure of information unrelated to the substance of the message.[58] Thus, an Internet service provider may divulge the identity of the author of an e-mail without violating the statute because the identity of the author does not qualify as content under the ECPA.[59]

The disclosure provision also contains exceptions. A service provider may disclose the contents of a message to the intended recipient of the communication[60] or to others with the lawful consent of the originator or intended recipient.[61] The exceptions also permit disclosure to employees of a communications service provider whose facilities forward the communication to its destination.[62] In addition, a communication service provider may disclose the contents of a message when such disclosure is "necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service."[63]

3. *Access to Stored Electronic Communications*

Finally, the ECPA forbids unauthorized access to stored electronic communications.[64] A violation occurs under this provision when, without permission, a person "obtains, alters or prevents authorized access to

---

56. The ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(A)–(B) (1994).

57. 18 U.S.C. § 2702(a)(1) (1994).

58. *See supra* notes 52–53 and accompanying text.

59. Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998).

60. 18 U.S.C. § 2702(b)(1) (1994).

61. 18 U.S.C. § 2702(b)(3) (1994).

62. 18 U.S.C. § 2702(b)(4) (1994).

63. 18 U.S.C. § 2702(b)(5) (1994).

64. 18 U.S.C. § 2701(a) (1994). For the ECPA definition of electronic storage, see *supra* note 56.

a[n] . . . electronic communication while it is in electronic storage."[65] However, the statute permits the person or company providing the electronic communication service to access stored electronic communications.[66] Indeed, this exception "allows service providers to do as they wish when it comes to accessing communications in electronic storage."[67]

B. Constitutional Privacy Protections in Washington

The Washington Constitution provides: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law."[68] The traditional approach to claims of constitutional privacy infringement, however, has been to focus primarily on the federal constitutional right of privacy,[69] which is triggered only by state action.[70]

Washington courts recognize two rights of privacy: the right to autonomous decisionmaking and the right to nondisclosure of personal information. Consistent with U.S. Supreme Court cases, Washington courts have recognized the right to autonomous decisionmaking as a "fundamental right."[71] The Supreme Court of Washington has strictly scrutinized government action that infringes upon the right to autonomous decisionmaking.[72] Under strict scrutiny analysis, the government must demonstrate some compelling governmental reason for infringing upon the fundamental right.[73] Nondisclosure of private information, however, is not treated as a fundamental right.[74] Because the right of nondisclosure is not fundamental, the court has applied a more

65. 18 U.S.C. § 2701(a).

66. 18 U.S.C. § 2701(c)(1) (1994).

67. Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (finding no violation of ECPA's prohibition against access to stored messages when city officials retrieved archived messages sent by city police officers over alphanumeric paging system because city was service provider under 18 U.S.C. § 2701(c)(1)).

68. Wash. Const. art. I, § 7.

69. *See, e.g.*, *In re* Colyer, 99 Wash. 2d 114, 120, 660 P.2d 738, 742 (1983) (deciding whether terminally ill adults have privacy right to refuse life support under Federal Constitution, but recognizing that Washington Constitution provides support for court's decision).

70. *Id.*

71. *See, e.g.*, O'Hartigan v. Department of Personnel, 118 Wash. 2d 111, 117, 821 P.2d 44, 47–48 (1991).

72. *Id.*

73. *Id.*

74. *Id.*

deferential "rational basis" analysis to the governmental activity.[75] Under the rational basis test, state action is permissible if the state articulates a legitimate governmental interest that the state action is designed to achieve.[76] The constitutional touchstone of the rational basis inquiry is not whether the state engaged in the least intrusive means possible, but whether the state engaged in activities appropriately tailored to further a legitimate state interest.[77]

Although the Washington Constitution protects against inappropriate state intrusion regarding decisionmaking and nondisclosure, some forms of private action might constitute "state action" under even the U.S. Constitution. For example, in the context of racial discrimination cases, federal courts may treat private conduct as state action if a claimed constitutional deprivation resulted from the actor's exercise of a state authorized right or privilege and if the court could fairly describe the acting party as a state actor.[78] The Court has relied on three factors in determining whether an actor qualifies as a state actor: the degree of reliance that the private actor has on governmental assistance and benefits, whether the private actor is providing a traditional governmental function, and whether the incidents of governmental authority uniquely aggravated the injuries suffered.[79] Although this analysis was designed to confront the question of state action in race discrimination cases, the analysis could apply in other contexts where state action is at issue.[80]

Some question exists as to whether state action is required to implicate the privacy right guaranteed by the Washington Constitution. The federal constitutional privacy right is not triggered unless "state action" occurs.[81]

---

75. *Id.*

76. *Id.* at 118, 821 P.2d at 48.

77. *Id.* at 118–20, 821 P.2d at 48–50 (upholding use of statutorily authorized polygraph testing to screen potential law enforcement employees despite availability of less intrusive means to obtain similar background information).

78. Lugar v. Edmonson Oil Co., 457 U.S. 922 (1982).

79. Edmonson v. Leesville Concrete Co., 500 U.S. 614, 618–28 (1991) (finding state action for equal protection purposes when private litigants in civil suit exercised peremptory challenges to exclude jurors based on race).

80. G. Sidney Buchanan, *A Conceptual History of the State Action Doctrine: The Search for Governmental Responsibility [Part II of II]*, 34 Hous. L. Rev. 665, 733 (1997).

81. Roe v. Wade, 410 U.S. 113, 153 (1973) (indicating that fundamental rights of privacy are founded "in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action"). Washington's interpretation of the right to privacy guaranteed under the Fourteenth Amendment to the Federal Constitution has more explicitly indicated the need for triggering state action. *In re* Colyer, 99 Wash. 2d 114, 120, 660 P.2d 738, 742 (1983).

However, Washington's constitutional privacy provision is not expressly limited to government conduct,[82] and the Supreme Court of Washington has refused to decide whether the state constitutional language protects against private action.[83] Moreover, the court has held that the speech and initiative clauses of the Washington Constitution, which are also phrased as rights of the people and not prohibitions against government, forbid even private action that intrudes on those rights.[84] Nevertheless, the court's interpretation of the speech and initiative clauses was based, in part, on the preferred status of the speech and initiative rights.[85] As a result, it remains unknown whether state action is required to trigger the privacy protection of the Washington Constitution, especially when non-preferred privacy rights are at issue.[86]

C. The Washington Privacy Act

Since 1909, the Washington Privacy Act has protected sealed messages, letters, and telegrams from being opened or read by someone other than the intended recipient.[87] More recently, the legislature expanded the protection to prohibit interception or recording of private conversations or communications transmitted by telephone, radio, or other point-to-point communications device.[88] This expansion created one of the most restrictive privacy acts in the nation.[89] Violations of any of these privacy protections may subject the violator to civil suit for damages, reasonable attorney's fees,[90] and even criminal charges.[91]

---

82. *See supra* note 68.

83. Doe v. Puget Sound Blood Ctr., 117 Wash. 2d 772, 783, 819 P.2d 370, 376 (1991) (indicating that whether wholly private conduct can violate state constitutional privacy right remains open question in Washington).

84. Alderwood Assocs. v. Washington Envtl. Council, 96 Wash. 2d 230, 243, 635 P.2d 108, 115–16 (1981).

85. *Id.* at 244–45, 635 P.2d at 116.

86. *See supra* note 83 and accompanying text.

87. Wash. Rev. Code §§ 9.73.010–.020 (1998).

88. Wash. Rev. Code § 9.73.030 (1998).

89. State v. Faford, 128 Wash. 2d 476, 481, 910 P.2d 447, 449 (1996).

90. Wash. Rev. Code § 9.73.060 (1998).

91. Wash. Rev. Code §§ 9.73.010–.030, .080 (1998).

1. *Protection of Sealed Messages*

Washington law prohibits the willful opening or reading of sealed messages, letters, and telegrams by persons other than the intended recipient.[92] This simply worded prohibition does not define some of its essential terms, such as "sealed" or "messages." However, in interpreting other undefined terms of the Privacy Act, the Supreme Court of Washington has consistently examined the ordinary meanings of undefined words.[93]

2. *Protection Against Use of a Device to Intercept or Record*

The Privacy Act also prohibits the use of a device to record or intercept private communications transmitted by telephone, telegraph, radio, or other point-to-point communications device.[94] Communications gain protection only if they can be classified as "private,"[95] which is determined by the intent and reasonable expectations of the parties to the communication.[96] The mere fact that a communication medium is not completely secure does not render conversations on that medium non-private.[97] Instead, the reasonableness standard requires a case-by-case inquiry into the surrounding circumstances and focuses primarily on the reasonable expectations of the parties involved.[98] Under such a reasonableness standard, a military tribunal found that an e-mail subscriber had a reasonable expectation of privacy in messages sent to other e-mail users with personally assigned passwords.[99]

---

92. "Every person who shall wilfully open or read, or cause to be opened or read, any sealed message, letter or telegram intended for another person . . . shall be guilty of a misdemeanor." Wash. Rev. Code § 9.73.020.

93. *Faford*, 128 Wash. 2d at 484, 910 P.2d at 451 (looking to English language dictionary when interpreting meaning of "privacy").

94. Wash. Rev. Code § 9.73.030(a).

95. *Faford*, 128 Wash. 2d at 484, 910 P.2d at 451.

96. *Id.*

97. The mere use of a cordless telephone did not undermine the clear intent of the parties to keep their telephone conversation private, despite the substantial potential for interception of the conversation. *Id.* at 485, 910 P.2d at 451.

98. *Id.* at 484–85, 910 P.2d at 451.

99. United States v. Maxwell, 42 M.J. 568, 576 (A.F. Ct. Crim. App. 1995), *rev'd on other grounds*, 45 M.J. 406 (C.A.A.F. 1996). Not all subjective expectations of privacy will meet the reasonableness test, however. For example, the Supreme Court of Washington held as a matter of law that answers given in response to questions asked by an unknown person over the telephone

No recording or interception takes place without the use of a recording or transmission device external to the communication.[100] For instance, no interception or recording occurs when a police informant tilts a telephone receiver so that a police officer can hear the conversation because the officer is merely listening to the sounds emanating from the original communication device.[101] Similarly, there is no interception or recording when one police officer listens on an extension line to a telephone conversation placed to another police officer, as there is no use of a recording or transmitting device separate from the telephone system used in the communication itself.[102]

III. FORMING THE REQUIRED REASONABLE BELIEF

The Washington anti-spam statute requires an ISP to have a reasonable belief that a message violates the statute before an ISP may block the message.[103] The statute, however, neither indicates what actions an ISP is entitled to take to form the requisite reasonable belief, nor limits those actions. The statute's silence on this point creates the possibility that different ISPs may rely on a variety of methods of obtaining reasonable belief. These various methods have different impacts on the e-mail subscriber's privacy.

A. Basic Components of E-mail Messages

The various methods of screening e-mail messages treat the component parts of the message differently, according to their function and content. Thus, to understand screening methods, one must first comprehend the components of an e-mail message. An e-mail message has three basic components: the header, the body, and the subject line.

The header of an e-mail message contains point-of-origin information.[104] Like the information contained on the outside of an envelope in which a letter is sealed, the header typically contains the name and

---

were not private. Kadoranian v. Bellingham Police Dep't, 119 Wash. 2d 178, 190–91, 829 P.2d 1061, 1067–68 (1992).

100. State v. Corliss, 123 Wash. 2d 656, 662, 870 P.2d 317, 320 (1994).

101. *Id.*

102. State v. Bonilla, 23 Wash. App. 869, 873, 598 P.2d 783, 786 (1979).

103. *See supra* note 34 and accompanying text.

104. Learn the Net, *LEARN THE NET: Anatomy of an E-mail Message* (last modified Mar. 22, 1999) <www.learnthenet.com/english/html/21e_anat.htm>.

electronic return address of the sender as well as the e-mail address of the intended recipient.[105] During delivery, the header accumulates electronic postmarks indicating the path that the letter has taken to reach its destination.[106]

The body of an e-mail message contains the message text.[107] In this regard, the body is roughly comparable to the contents of a regular letter. The body of the message is typically pure "content" and will rarely be useful to an ISP during delivery. It is conceivable, however, that an ISP might have a legitimate need to examine the content of an e-mail to determine where to route misdelivered e-mail.[108]

The subject line of an e-mail message contains text that briefly describes the body of the e-mail.[109] The subject line is similar to the "RE:" line of a memorandum and may be thought of as the title of the e-mail. Many e-mail browsers automatically display the subject line of an e-mail in the inbox, even before the user "opens" the message. In that sense, the information contained in the subject line seems more visible and open to view, and is therefore similar to the header information. The subject line usually contains a summary of the body "content,"[110] making it similar to the body of an e-mail message.

B. Three ISP Approaches to Forming Reasonable Belief

An ISP seeking to form a reasonable belief under the anti-spam statute may treat the various components of e-mail messages differently, based on differences in the content and function of those components. Consider the following three approaches a receiving ISP might take to form the required reasonable belief.[111]

---

105. *Id.*

106. *Id.*

107. *Id.*

108. Ian C. Ballon, *Linking, Framing and Other Hot Topics in Internet Law and Litigation*, 520 PLI/Pat. 167, 295 (1998).

109. Technically, the subject line may be considered part of the header of an e-mail message. Learn the Net, *supra* note 104. However, because the subject line contains content, this Comment treats the two concepts as distinct.

110. The subject line contains "content," at least as the ECPA defines that term. *See supra* note 52 and accompanying text. While the ECPA definition is not directly applicable in the context of the Privacy Act, the ECPA does seem to provide some assistance in determining the type of protection the subject line should receive.

111. The following approaches focus on the potential activities of a receiving ISP. *See, e.g.*, *infra* note 113. However, sending and foreign ISPs might also rely on variations of the three

First, a receiving ISP might choose to rely solely on the prior experiences of its customers. The Washington Attorney General interprets the anti-spam statute as allowing ISPs to form the requisite reasonable belief by relying on past subscriber complaints about a sending party.[112] For instance, if a receiving ISP learns that its customers received messages from "nobody@nowhere.com" in violation of the statute, the receiving ISP may refuse to deliver any future message from that address or domain name. Under such an approach, the ISP could rely solely on subscriber complaints to determine whether commercial e-mail violations have occurred and could develop a blacklist of offenders whose e-mail would be subject to automatic blocking.[113] This approach only requires an examination of e-mail header information to see if the sending party is a known offender and requires no examination of the subject line or body of any given message.[114]

Second, an ISP might choose to develop affirmatively its reasonable belief by relying on active content monitoring. Under this "proactive approach," the ISP actively verifies point of origin information and confirms the accuracy of subject lines. The ISP would verify the consistency of the identifying information in the header to determine the accuracy of point of origin information.[115] The ISP would then examine the content of the message to determine whether it qualifies as commercial mail. To verify the accuracy of the subject line, the receiving ISP would rely on either sophisticated software or the watchful eye of an

---

described approaches in trying to enforce the statute. In one case, a sending ISP discontinued service to its own e-mail subscriber because of costs that the subscriber's bulk e-mailing imposed on the ISP. Cyber Promotions, Inc. v. Apex Global Info. Servs., Inc., No. Civ.A. 97-5931, 1997 WL 634384, at *2 (E.D. Pa. Sept. 30, 1997) (issuing preliminary injunction requiring ISP to continue providing service to bulk e-mailer).

112. "Once an ISP has reason to believe their [sic] network is being used to send unlawful unsolicited commercial e-mail, they [sic] can block all further e-mail sent to its subscribers from the address or domain name of the subscriber." Attorney Gen. of Wash., *supra* note 25.

113. *See, e.g.*, CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019 (S.D. Ohio 1997) (refusing to prohibit national ISP's use of software programs to filter out messages of particular commercial e-mail sender when filtering began only after substantial customer complaints).

114. This approach assumes that an ISP can reasonably believe that all future e-mail messages from a blacklisted sender will contain false or misleading information and will be commercial in nature. The Attorney General of Washington apparently endorses this assumption. *See supra* note 112.

115. For instance, software could check to ensure that the sender's address, the return address, and the sending ISP's domain name are consistent.

ISP employee to compare the subject lines to the bodies of incoming e-mail messages.[116]

A third approach might combine aspects of the proactive and reactionary approaches. This "hybrid approach" would actively monitor point of origin information for violations, but would not actively monitor the subject line of messages, out of respect for the user's privacy. Instead, the ISP would reactively rely on subscriber complaints as the source of its reasonable belief that a particular message violates the subject line prong of the anti-spam law. This portion of hybrid monitoring is consistent with the reactionary approach and, like that approach, would rely solely on past subscriber complaints. The other portion of hybrid monitoring engages in active monitoring of point of origin information contained within the header. The ISP also must form a reasonable belief that a given message is "commercial,"[117] because active enforcement of the point of origin prong of the statute requires no prior history with the sending party. Thus, ISPs relying on the hybrid approach must actively scan some content-laden portion of e-mail messages that contain misleading point of origin information to develop a reasonable belief that those messages are commercial in nature.[118]

IV. EXISTING PRIVACY PROTECTIONS ARE INSUFFICIENT

A. Numerous Exceptions to ECPA Provisions Render the Statute Ineffective in Preventing ISPs from Screening E-mail Content

The federal ECPA's provisions regarding interception of, access to, and disclosure of electronic communications provide little protection for e-mail subscribers whose ISPs choose to inspect their e-mail messages for violations of the Washington anti-spam law. The ECPA's prohibition of interception affords the greatest potential privacy protection to e-mail subscribers from ISP monitoring activities. However, ISPs can sequence

116. Although ISPs handle large volumes of e-mail, existing computer software can scan for incoming e-mail messages of interest, based on the sender's address, keywords in the subject line or body of the e-mail, or other information contained in the e-mail. If the software determines that a message is suspicious, the software can save the message for later human examination. Jim Heath, *Survey: Corporate Uses of Cryptography* (visited Mar. 12, 1999) <http://www.iinet.net.au/~heath/crypto.html>.

117. *See supra* note 17 and accompanying text.

118. Perhaps ISPs could assess whether messages are commercial without examining the content of the messages. However, it seems more likely that this assessment requires active investigation of at least the subject line.

their activities to completely avoid the interception provision. Although the ECPA also prohibits disclosure and access, the exceptions to those prohibitions render the ECPA completely ineffective against unwelcome ISP content monitoring.

1. ISPs Can Avoid ECPA's Interception Provision by Carefully Sequencing Their Activities

The ECPA's prohibition against interception of electronic communications can be completely sidestepped by careful ISP activity. Reactionary monitoring fully conforms to ECPA's prohibition on interception. Activities associated with the proactive and hybrid approaches, on the other hand, qualify as interceptions. By sequencing their activities, ISPs engaging in proactive and hybrid approaches can circumvent the interception provision altogether.[119]

An ISP can pursue a reactionary approach without running afoul of the ECPA's protection against interception. Interception occurs when there is nonconsensual acquisition of the substance of an electronic communication not necessary for providing electronic communication service.[120] When an ISP examines the header of an e-mail message pursuant to a reactionary approach, the ISP is examining a portion of the message that contains information identifying the sending and receiving parties, and such information is not considered content under the ECPA.[121] Moreover, an ISP must have access to sender and recipient information as a necessary incident to providing e-mail services. Thus, the reactionary approach conforms to the requirements of the ECPA.

ISPs that engage in proactive or hybrid approaches may run afoul of the ECPA's interception prohibition. Under this provision, ISPs may not examine the contents of e-mail messages during transmission, which terminates when a message has been stored for retrieval.[122] Active and hybrid approaches, by their nature, require ISPs to examine the subject line and/or body of e-mail messages. This examination qualifies as an acquisition of the substance of the e-mail communication,[123] and such

---

119. Such sequencing is technologically feasible using existing software technology. *See supra* note 116.

120. *See supra* notes 52, 54–55 and accompanying text.

121. *See supra* note 53 and accompanying text.

122. *See supra* note 51 and accompanying text.

123. *See supra* note 110.

acquisition is unnecessary to providing Internet service.[124] Thus, proactive or hybrid ISP monitoring that occurs before a message is saved for retrieval probably qualifies as interception under the ECPA.

ISPs that choose the active or hybrid approaches probably do not meet the requirements of the protection of interests exception to the interception provision. The ECPA permits interception by a communications service provider when such interception is necessary to protect the rights or property interests of the provider.[125] Active monitoring protects the ISP's statutory right to block violative e-mail messages. It also protects the ISP's property interests by relieving the ISP from the burden of processing, storing, and transmitting false or misleading e-mail messages, which are often sent in bulk quantities.[126] While active monitoring may be useful in protecting ISP rights and property interests, such monitoring is unnecessary because ISPs can employ less intrusive approaches, like the reactionary approach, to protect their rights. Because active monitoring is not necessary to protect ISP rights or property, ISPs probably will be unsuccessful in arguing that active monitoring meets the requirements of this exception.[127]

ISPs can nevertheless avoid the interception inquiry entirely by first saving incoming messages for retrieval and then examining the saved version of the message to search for violations. This is because the ECPA provision against interception applies only if the message has not been stored for retrieval.[128] If the ISP has first saved the message for retrieval, the ISP's subsequent access to the stored message is completely unrestricted.[129] Thus, an ISP could circumvent this provision merely by carefully sequencing its activities.

---

124. The Washington anti-spam law permits ISPs to voluntarily block violative e-mail messages but does not require them to do so. *See supra* note 34 and accompanying text. The mere fact that inspection of the contents of incoming e-mail messages might be useful to the ISP in determining whether to block e-mail should not transform it into a necessary incident to providing e-mail service. Aside from enforcing the anti-spam law, an ISP will rarely, if ever, need to examine the contents of an e-mail message to provide e-mail service to its subscribers. *But see supra* note 108 and accompanying text (indicating that examining e-mail content may occasionally prove helpful in e-mail delivery).

125. *See supra* note 55 and accompanying text.

126. *See supra* note 11 and accompanying text.

127. This interpretation is consistent with the statute's express prohibition on continuous monitoring of wire communications when such monitoring is not related to mechanical or service quality control checks. 18 U.S.C. § 2511(2)(a)(i) (1994).

128. *See supra* note 51 and accompanying text.

129. *See infra* notes 134–35 and accompanying text.

2. *Message Content May Be Revealed to ISP Employees Under an Exception to ECPA Disclosure Rules*

The ECPA's prohibition against disclosure does not forestall any of the three approaches to developing a reasonable belief because the ISP activities envisioned by those approaches fall within the recognized exceptions. The ECPA prohibits electronic communication providers from disclosing the contents of a stored message to unauthorized parties, except as is necessary to provide the service or to protect the provider's rights and property interests.[130] Because the reactive approach requires no examination of message content,[131] it does not violate the disclosure provision. Conversely, the active and hybrid approaches envision disclosure of message content to computer software and potentially to ISP employees. Although the statute permits disclosure when necessary to protect the rights of a service provider,[132] the rights of the ISP can be adequately protected by other methods that do not require disclosure. Another exception to this prohibition, however, specifically permits disclosure to a person employed at a facility used to forward the communication.[133] Because an e-mail provider employs the person who ultimately examines the message content, the employee's examination of the message would satisfy the exception. Thus, the active and hybrid approaches under the anti-spam law do not violate the provisions prohibiting ISPs from disclosing the contents of stored messages.

3. *ECPA Places No Restriction on ISP Access to Stored Messages*

E-mail subscribers would have an even more difficult time advancing claims against ISPs under the ECPA's prohibition of unauthorized access to stored electronic communications. By examining the contents of a stored e-mail message, an ISP accesses stored electronic communications.[134] However, the statute creates a blanket exemption from the access prohibition for the communications service provider, allowing ISPs to do

130. *See supra* notes 54–55 and accompanying text.

131. *See supra* notes 113–14 and accompanying text.

132. *See supra* note 63 and accompanying text.

133. *See supra* note 62 and accompanying text.

134. By accessing and examining the e-mail, the ISP "obtains" the e-mail and by refusing to deliver the message to its recipient, the ISP "prevents authorized access to" the e-mail. *See supra* notes 64–65 and accompanying text.

as they please when it comes to accessing stored communications.[135] Because of this blanket exemption, the statute does not restrict the approaches that an ISP could use under the anti-spam statute.

B. ISPs May Constitutionally Monitor E-mail Because They Are Not State Actors and Their Actions Are Supported by a Rational Basis

Existing law recognizes that violations of Washington's constitutional right to privacy occur when government action intrudes upon a person's private affairs.[136] The anti-spam statute only authorizes ISPs to "voluntarily" block the transmission or receipt of messages reasonably believed to violate the statute; it does not mandate such action.[137] It is doubtful that Washington courts will agree that an ISP has engaged in state action by voluntarily pursuing any of the three approaches to developing reasonable belief.

Government action may occur when the government has authorized the conduct at issue and private actors have voluntarily acted, as long as courts can fairly characterize the actor as a state actor.[138] Under the anti-spam law, however, the question about the appropriateness of the three approaches arises because the State has not explicitly authorized any methods for forming reasonable belief.[139] Because ISPs pursue active or hybrid approaches without government authorization, the ISP activities do not disturb the constitutional protection of privacy from government intrusion.[140]

If ISP content monitoring does not qualify as state action, such monitoring probably will escape constitutional scrutiny altogether. The Supreme Court of Washington has yet to decide whether the Washington Constitution prohibits private action that intrudes on the right to

---

135. *See supra* notes 66–67 and accompanying text.

136. *See supra* note 69 and accompanying text.

137. *See supra* note 34 and accompanying text.

138. *See supra* note 78 and accompanying text.

139. *See supra* Part I.B.

140. The anti-spam statute does not authorize ISPs to inspect e-mail messages but does authorize ISPs to block violative e-mail messages. Because e-mail blocking is a state-authorized activity, ISPs engaged in blocking might meet the description of a state actor. ISPs provide a service that is very similar to a traditional governmental service by serving as an electronic post office. Moreover, the incidents of government authority might uniquely aggravate the injury by virtue of the no-liability protection for ISPs who act pursuant to the statute in good faith. *See supra* note 79 and accompanying text.

nondisclosure.[141] The court has decided that private action can violate the speech and initiative clauses of the Washington Constitution[142] because of the preferred status of the speech and initiative rights.[143] The right to nondisclosure, on the other hand, is not considered a fundamental or preferred right,[144] so Washington courts are unlikely to find a constitutional violation when an ISP engages in content monitoring that amounts to only private action.[145]

Even if a court agrees that the ISP's act of examining an e-mail somehow constitutes state action, that court still would need to decide whether to apply strict scrutiny or rational basis analysis to the state action.[146] Strict scrutiny applies to state actions infringing upon the rights to personal autonomy and decisionmaking, because those rights are given fundamental status under the Washington Constitution.[147] Washington courts apply rational basis scrutiny to non-fundamental rights, such as the right to nondisclosure of personal information.[148] Given the judiciary's reluctance to extend the class of fundamental rights of privacy, courts probably will favor an application of the rational basis test to ISP examination of private e-mail messages. Moreover, the subscriber's right to receive e-mail without disclosure of the contents more closely resembles the right to nondisclosure of personal information than the fundamental rights to freedom and autonomy in decisionmaking. Because the privacy right in e-mail delivery does not implicate a fundamental right, state action that intrudes on that right must only satisfy the rational basis test.[149]

Therefore, the final question in this privacy analysis is whether there is a neutral and legitimate government interest that suffices as a rational

---

141. *See supra* note 83.

142. *See supra* note 84.

143. *See supra* note 85 and accompanying text.

144. *See supra* note 74 and accompanying text.

145. The Supreme Court of Washington is more likely to interpret the constitutional privacy protection to prohibit private action that infringes upon fundamental rights, such as the right to autonomous decisionmaking, because of the importance of those rights. *See* O'Hartigan v. Department of Personnel, 118 Wash. 2d 111, 117–18, 821 P.2d 44, 47–48 (1991) (refusing to classify nondisclosure of personal information as fundamental privacy right).

146. *See supra* note 71 and accompanying text.

147. *See supra* notes 71–73 and accompanying text.

148. *See supra* notes 74–76 and accompanying text.

149. *See supra* notes 74–75, and accompanying text.

basis to authorize the conduct.[150] Provided that the government can demonstrate a rational basis for intruding on the particular privacy right, the state action is permissible even when less intrusive methods exist to obtain similar information.[151]

The legislative findings of the anti-spam law indicate that the legislature intended to provide immediate relief to ISPs from the heavy burden of carrying e-mail messages with false or misleading points of origin.[152] The findings do not specifically indicate the rationale for allowing ISPs to block messages with false or misleading information in the subject line.[153] Nonetheless, such a policy furthers a legitimate governmental interest by fostering confidence among e-mail subscribers that commercial e-mails are accurate, reducing the burdens on ISPs,[154] and abating the burden on the Attorney General's office in responding to consumer complaints about commercial e-mail. These governmental interests provide sufficient and rational bases that permit the government to intrude on the nondisclosure privacy right of e-mail subscribers. Furthermore, because active content monitoring could be expected to produce more effective enforcement of the anti-spam law than reactionary or hybrid approaches, a rational basis exists to support the use of proactive methods, despite the existence of less intrusive approaches.

C. *Message Screening Does Not Violate the Washington Privacy Act*

Although the Washington Privacy Act has been labeled one of the most restrictive privacy acts in the nation,[155] the protection is illusory to e-mail subscribers seeking protection from unwarranted intrusions by their ISPs. The Act's protection of sealed messages does not apply to most e-mail messages because they are not sufficiently "sealed." The various exceptions to the Act's prohibitions render the Act completely ineffective against the contemplated ISP activities. Thus, the high wall of

150. *See supra* note 76 and accompanying text.

151. *See supra* note 77 and accompanying text.

152. *See supra* note 15 and accompanying text.

153. The legislative findings state that "the consumer protection division of the attorney general's office reports an increasing number of consumer complaints about commercial electronic mail." Wash. Rev. Code § 19.190.005 (1998). However, nothing in the statute itself ties these consumer complaints to the provisions allowing ISPs to block messages with false or misleading information in the subject line.

154. *See supra* notes 9–11 and accompanying text.

155. *See supra* note 89 and accompanying text.

privacy created by the Washington Privacy Act is nevertheless one that an ISP can easily surmount and does not protect users from ISPs that choose to engage in active content monitoring.

1. The Act's Sealed Messages Provision Does Not Protect Most E-mail Messages Because They Are Not "Sealed"

The Washington Privacy Act prohibits unauthorized parties from opening or reading sealed messages.[156] When construing the provisions of the Privacy Act, the Supreme Court of Washington has interpreted undefined statutory language in its ordinary and usual meaning.[157] E-mail undoubtedly falls under the general rubric of "messages" as that word is commonly used.[158]

Although e-mail communications qualify as "messages," it is not as clear whether e-mail messages are "sealed." Most e-mail users send their messages in unencrypted form,[159] exposing their messages to the view of others while they travel through cyberspace. In this respect, e-mail resembles an unsealed postcard more than a sealed letter.[160] However, even unencrypted e-mail messages are severed into packets before being transmitted across the Internet.[161] Those packets often travel along different routes toward their destination, where the packets are finally reassembled into the complete e-mail message.[162] Given the difficulties of locating these packets during transit and reassembling them into the complete e-mail message, would-be interceptors can only feasibly intercept e-mail messages at the sender's or the recipient's host

156. *See supra* note 92 and accompanying text.

157. *See supra* note 93 and accompanying text.

158. Courts commonly refer to e-mail communications as e-mail messages. *See, e.g.*, Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105, 1106 (E.D. Mich. 1998); Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998); Wesley College v. Pitts, 974 F. Supp. 375, 380 (D. Del. 1997); Bonamy v. City of Seattle, 92 Wash. App. 403, 407, 960 P.2d 447, 450 (1998).

159. Encryption is a process by which a computer encodes the text of e-mail messages into unintelligible symbols to prevent intercepting parties from determining the content of the message. By use of a translation "key," the receiving computer can decrypt the message for reading. For an easy-to-read explanation of basic encryption technologies, see generally Heath, *supra* note 116.

160. Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 Harv. L. Rev. 1591, 1597 (1997).

161. *Id.*

162. *Id.*

computers.[163] Because packets effectively conceal the content of the message during transmission, a court could conclude that the message is sealed during transmission. Once the packets arrive at the recipient's host computers for reassembly, the message again becomes exposed to viewing in its entirety and loses any protection that the packet-wise transmission might have conferred upon it. Because a receiving ISP examines a message upon receipt and only after the message is reassembled, the sealed message provision of the Privacy Act would not forestall ISPs from engaging in active content monitoring.

A less technical assessment of what constitutes effective sealing also would permit ISPs to engage in active content monitoring of most messages. One court observed, "Unlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)."[164] Under such an analysis, only encrypted e-mail messages meet the sealed message requirement and unencrypted mail messages receive no protection.[165]

Although the Act may give privacy protection to the concealed portions of encrypted messages, the Privacy Act provides no protection to unencrypted messages once ISPs receive the messages for delivery. ISP monitoring of unencrypted messages can range from the reactionary approach to the proactive approach without running afoul of the sealed messages provision of the Privacy Act.

2. *Message Screening Does Not Violate the Interception or Recording Provisions of the Act Because ISPs Use No "External Device"*

The Privacy Act also protects point-to-point e-mail communications. Specifically, it prohibits the interception or recording of such communications by the use of some device external to the communication.[166] E-mail can constitute a "[p]rivate communication transmitted by telephone . . . or other device between two or more

163. *Id.*

164. ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996).

165. Encryption also makes it impracticable for ISPs to engage in active monitoring because modern encryption securely conceals the content of the e-mail message. Ironically, the encryption process that can transform an e-mail into a "sealed" message is the same process that renders the e-mail's "sealed" status unnecessary because ISPs would become unable to examine the message content.

166. *See supra* note 94 and accompanying text.

individuals."[167] E-mail communication is generally a communication between at least two people by use of computers. The Act protects only "private" communication, as demonstrated from a fact-specific inquiry into the intent and reasonable expectations of the parties.[168] Because of the fact specificity of the inquiry, it is difficult to predict in any generalized sense whether e-mail messages will meet the test. However, courts should find, in the appropriate circumstances, that the parties to an e-mail message reasonably expected the contents of the message to remain private. One military tribunal has found that an e-mail subscriber had an objectively reasonable expectation of privacy in messages sent to other e-mail users with individually assigned passwords.[169] Such a message should meet the privacy requirement of the Privacy Act. On the other hand, commercial e-mail messages sent to thousands of e-mail accounts would probably not satisfy the privacy requirement because the sender could not reasonably believe that the message would remain private.[170]

When an ISP blocks the transmission of an e-mail message, it effects an interception under the Privacy Act. Despite this interception, the anti-spam law specifically relieves ISPs from liability for blocking messages they reasonably believe violate the anti-spam law.[171] Thus, as long as the ISP formed a reasonable belief and acted in good faith upon that belief, the more recently enacted provisions of the anti-spam statute render the Privacy Act's provisions against interception inapplicable to an ISP's decision to block e-mail messages.[172]

Proactively monitoring the subject line and points of origin of e-mail messages does not result in an interception or recording under the Privacy Act because no interception or recording occurs without the use of some device external to the communication.[173] When an ISP actively monitors

167. Wash. Rev. Code § 9.73.030(1)(a) (1998).

168. *See supra* notes 98–99 and accompanying text.

169. United States v. Maxwell, 42 M.J. 568, 575 (A.F. Ct. Crim. App. 1995), *rev'd on other grounds*, 45 M.J. 406 (C.A.A.F. 1996). *Maxwell* does not decide whether it is also reasonable to expect privacy in messages sent over the Internet, where messages are more susceptible to being viewed and intercepted.

170. E-mail sent to numerous strangers seems roughly analogous to telephone conversations with total strangers, which have been determined not to be private as a matter of law. Kadoranian v. Bellingham Police Dep't, 119 Wash. 2d 178, 190–91, 829 P.2d 1061, 1067–68 (1992).

171. *See supra* note 35.

172. The provision against recording or intercepting communications remains an important check against bad faith actions that ISPs might take. For that reason, ISPs should be wary about abusing their power under the statute.

173. *See supra* note 100 and accompanying text.

subject line and origination information, it is using the same computer system as the communication it is monitoring and, applying the same logic as the extension telephone cases,[174] should not constitute an interception or recording. Because these monitoring practices use no device external to the e-mail communication, no interception or recording occurs.

V. THE WASHINGTON ANTI-SPAM LAW SHOULD BE AMENDED TO LIMIT ISP ACTIVITIES

Existing privacy protections fall miserably short of protecting e-mail subscribers from intrusive ISP activities. Privacy law permits ISPs to take even the most active steps of examining the body of e-mail messages addressed to private subscribers if they so choose. Given the permissiveness of current privacy protections, the Washington Legislature should reassess and revise the anti-spam statute. The revisions should include explicit provisions prohibiting ISPs from actively monitoring the content of messages. Such a revision would safeguard the privacy rights of e-mail consumers, while retaining adequate protection for the legitimate property interests of ISPs.

A careful review of the legislative findings makes it clear that when the legislature passed the anti-spam law, it was attempting to remedy the problems of ISPs.[175] Admittedly, many e-mail subscribers may share the concerns of their ISPs about the growing volume of commercial e-mail. E-mail subscribers also benefit from the statute's provisions that enable the recipients of violative e-mail messages to sue the sender.[176] Whatever protections the statute gives to users from abusive e-mail senders, the statute makes no attempt to protect users from the activities of their own ISPs. This lack of concern for user privacy from ISP monitoring is not surprising, given that the legislature enacted the anti-spam statute to protect the interests of ISPs.

The legislature easily could rectify the oversight by amending the anti-spam statute to include specific limitations on the permissible actions of ISPs seeking to form a reasonable belief that a message violates the anti-spam law. Existing federal law permits the legislature to endorse the reactionary, the hybrid, or the proactive approaches (or any combination of

174. *See supra* notes 101–02 and accompanying text.

175. *See supra* note 15 and accompanying text.

176. *See supra* note 29 and accompanying text.

the three) when forming a reasonable belief.[177] The constitutional protection of privacy rights also permits the legislature to sanction any of the three approaches.[178] Although such an endorsement would constitute state authorization of intrusions on the right to nondisclosure of e-mail messages, the authorization would need to satisfy only a rational basis inquiry.[179]

Specifically, the legislature should amend the anti-spam statute so that it prohibits ISPs from examining the contents of e-mail messages and limits ISPs to the reactionary approach to implementing the anti-spam statute.[180] As the law currently reads, ISPs can actively scan the content of e-mail messages under the hybrid and proactive approaches and incur no liability for doing so if they act in good faith on their reasonable beliefs. Under this proposed amendment, ISPs could only develop a reasonable belief by way of past subscriber complaints.[181] Furthermore, if an ISP overreached its authority by engaging in active content monitoring, the ISP would lose its shield from liability because it failed to make good faith efforts to comply with the statute. These changes would clarify the role of ISPs under the anti-spam law and prevent ISPs from overexerting their authority.

Recall the Samantha and Roger hypothetical discussed in the beginning of this Comment. At present, neither Samantha nor Roger has a valid claim against Roger's ISP, despite the ISP's use of active content monitoring to form a reasonable belief that Samantha's e-mail violated the anti-spam statute. The ISP properly sequenced its activities to avoid the only non-excepted provision of the ECPA. The ISP is probably not a state actor and, even if it is, the ISP could postulate a rational basis for its activities. Finally, the ISP did not open or read a "sealed" message as that term is defined under the Washington Privacy Act and did not use any device external to the e-mail communication to intercept or record Samantha's and Roger's communication.

---

177. ISPs qualify under exceptions to the disclosure and access provisions of the ECPA and can sequence their activities to avoid the ECPA's prohibition of interception of electronic communications. *See supra* Part IV.A.1.

178. The right implicated by all three approaches is the privacy right against disclosure, so the "rational basis" test applies. ISP active content monitoring surely meets that low standard. *See supra* Part IV.B.

179. *See supra* notes 74–75 and accompanying text.

180. Although the Attorney General has not expressed a position as to the limitations on ISPs in forming a reasonable belief, the passive approach is the only approach that the Attorney General has affirmatively endorsed. *See supra* note 112.

181. *See supra* notes 113–14 and accompanying text.

Under the proposed amendment, however, Samantha and Roger would have a valid cause of action. Roger's ISP did not believe that Samantha was a known violator of the anti-spam law, as revealed by customer complaints. Instead, Roger's ISP relied on the proactive approach of active content monitoring. Because the proposed amendment to the anti-spam statute would unambiguously forbid such content monitoring, Roger's ISP could not have acted in good faith reliance on the anti-spam statute and would not qualify for protection from liability. Roger and Samantha could both sue for damages incurred as a result of the examination and the blocking. By amending the anti-spam law, the legislature can protect the rights of individual e-mail subscribers like Roger and Samantha more effectively while still allowing ISPs the right to protect their property interests.

VI. CONCLUSION

ISPs should not be dragooned into service by free-riding entrepreneurs. At the same time, e-mail subscribers should retain a sphere of privacy in their e-mail communication. The legislature must strike an appropriate balance between these competing interests. In part, the Washington anti-spam statute attempts to address ISP and subscriber concerns by creating civil penalties for those who send false or misleading e-mail messages. The legislature also empowered ISPs with the right to block messages reasonably believed to violate the statute. This blocking provision, coupled with a complete statutory silence on the issue of how an ISP is to determine when an e-mail violates the statute, poses a substantial threat to the e-mail subscriber's privacy right. An evaluation of existing state and federal privacy protections reveals that even the most intrusive ISP activities of active monitoring are not prohibited. Fortunately, the legislature can restore the privacy rights of e-mail subscribers by passing an amendatory clarification of the limits on ISP activities in determining whether a particular e-mail message violates the anti-spam statute. The legislature should permit ISPs to block messages based on prior complaints of their subscribers and should prohibit ISPs from actively monitoring the content of incoming and outgoing messages. Such a limitation will best effectuate the interests of e-mail subscribers and ISPs alike.